INSERT COIN

BOTNETS

Taller de Informatica Forense

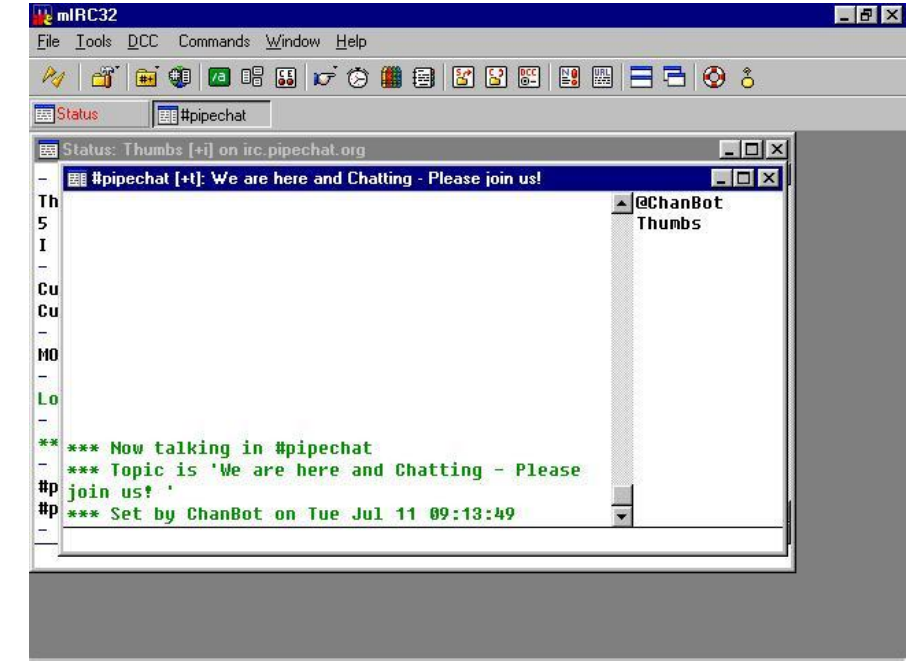
matias porolli
utn

2011

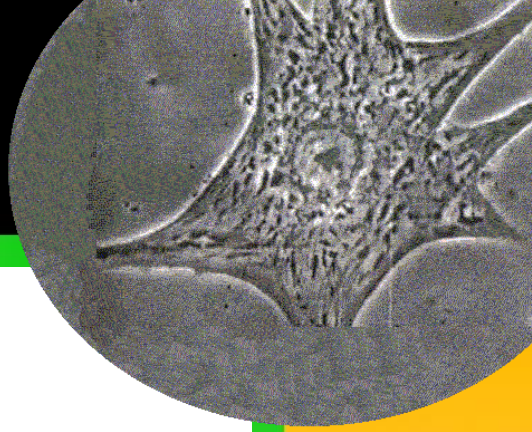
Historia

1988 IRC

- Chat grupal / individual
- Cliente – Servidor
- Administradores



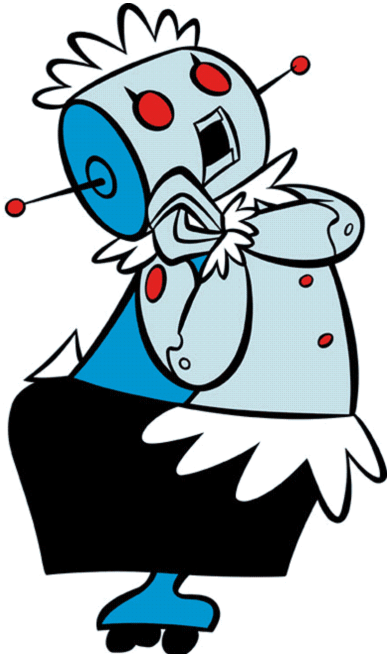
Historia



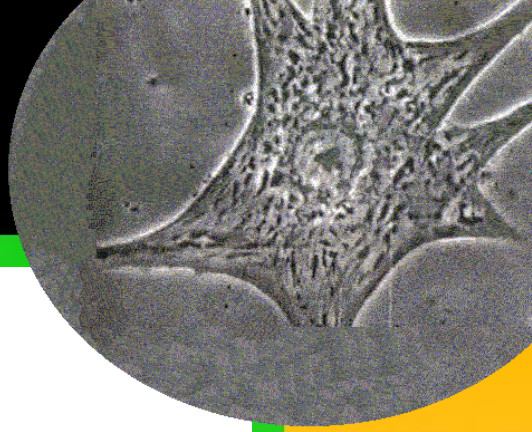
1989GM

- Uno de los primeros bots
- Bot: script que se comporta como usuario
- Juega “Caza al Wumpus” contra humanos

- Remplazar al administrador
- Realizar tareas rutinarias



Historia



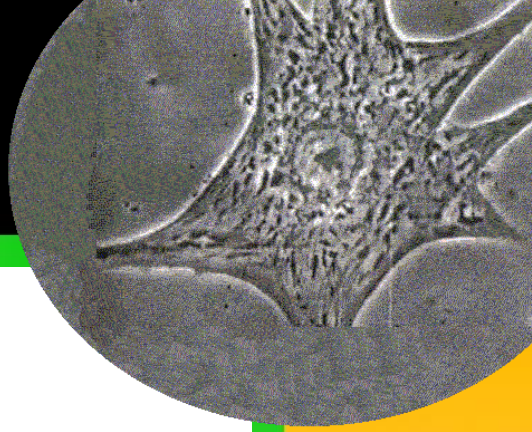
1999 Pretty Park

- Código Malicioso: gusano
- Obtiene info del sistema
- Realiza harvesting
- Descarga de archivos

1999 SubSeven

- Código Malicioso: troyano
- Permite control del sistema

Historia

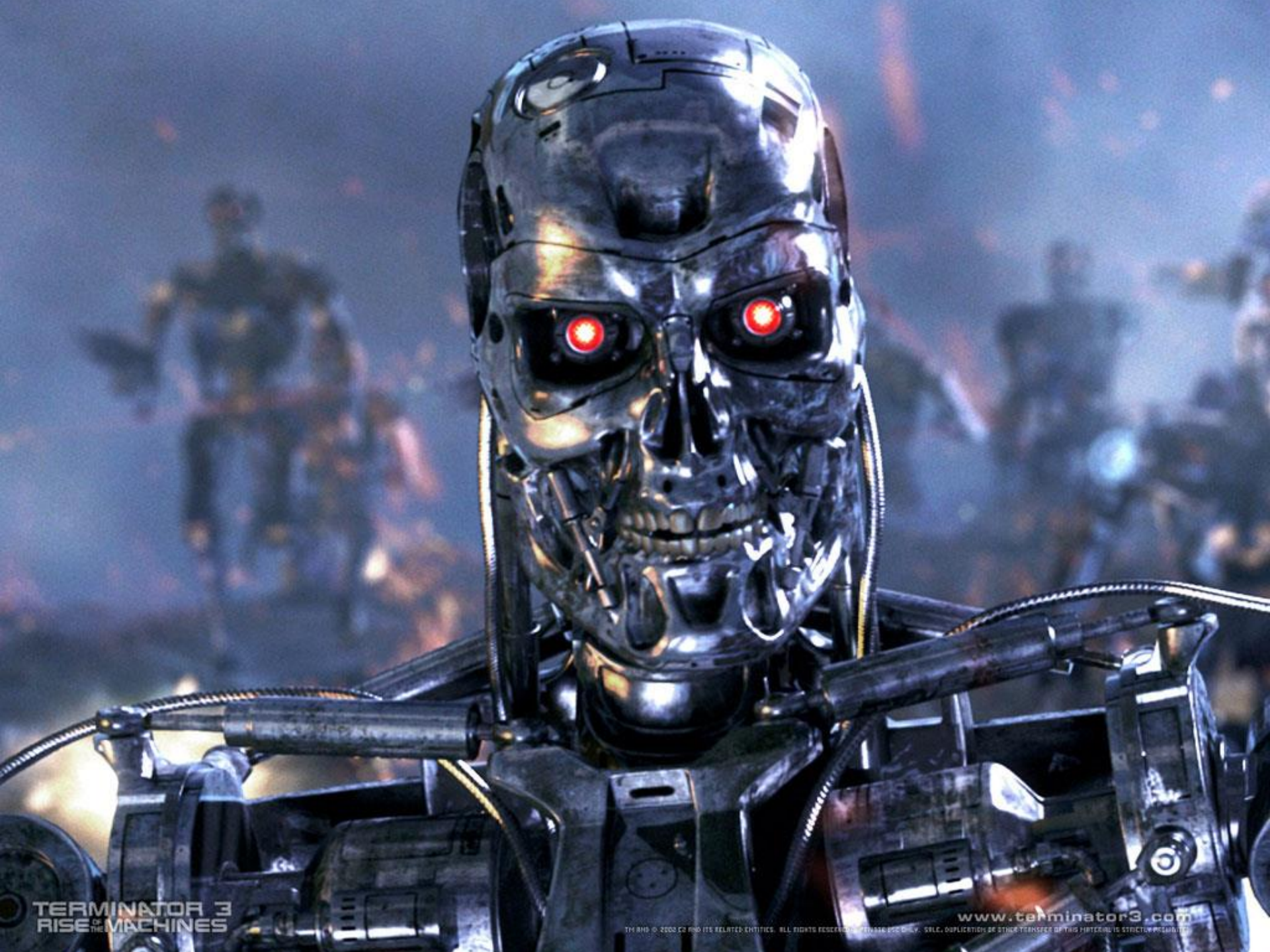


_-_-Ideas básicas

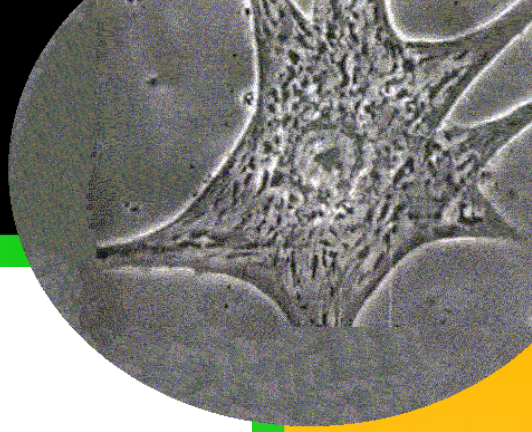
- Medio de Comunicación y Control
- Bot escucha canal IRC, espera comandos
- Control remoto, automatización
- Descarga de archivos

_-_-Código malicioso

- Antes: diversión, conocimiento, reto
- Ahora: $$$, crimen, mafia


TERMINATOR 3
RISE OF THE MACHINES
www.terminator3.com

Historia



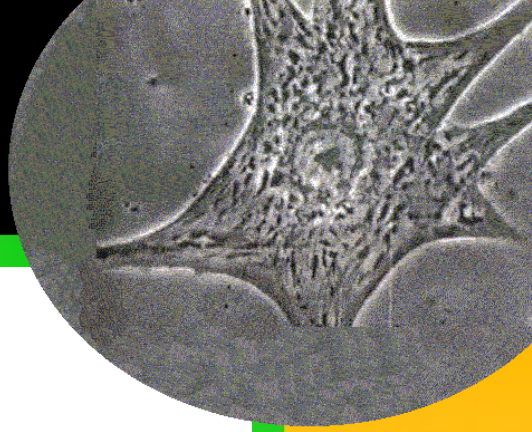
2000 GT Bot

- Basado en mIRC
- Oculta su presencia en el sistema
- Ejecución remota de procesos
- Acceso anónimo al servidor IRC

2002 SDBot

- De código abierto
- Muy simple
- Da lugar a cientos de bots similares con distintas funciones

Historia



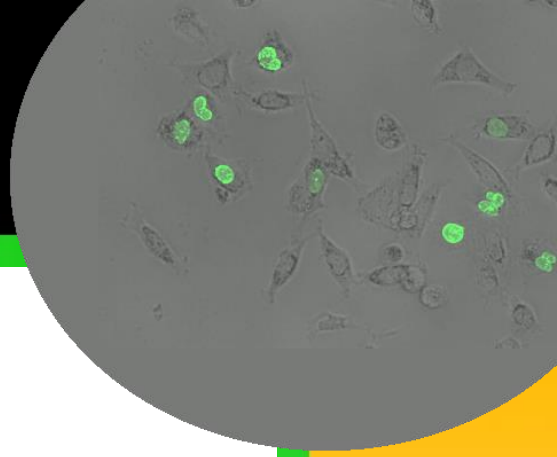
2002 Agobot

- Diseño modular
- Los módulos se obtienen por etapas

Por ejemplo:

- Módulo 1: cliente IRC, backdoor
- Módulo 2: mata procesos antivirus
- Módulo 3: bloquea acceso sitios web
- Módulo n: payload

Conceptos



>Bots

- Programas que automatizan tareas

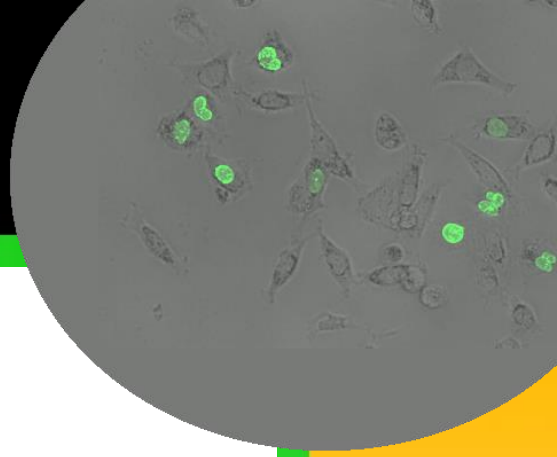
>Zombies

- Computadoras infectadas por el bot

>Botnets

- Redes de zombies controlados en forma remota
- Sin consentimiento o conocimiento

Conceptos

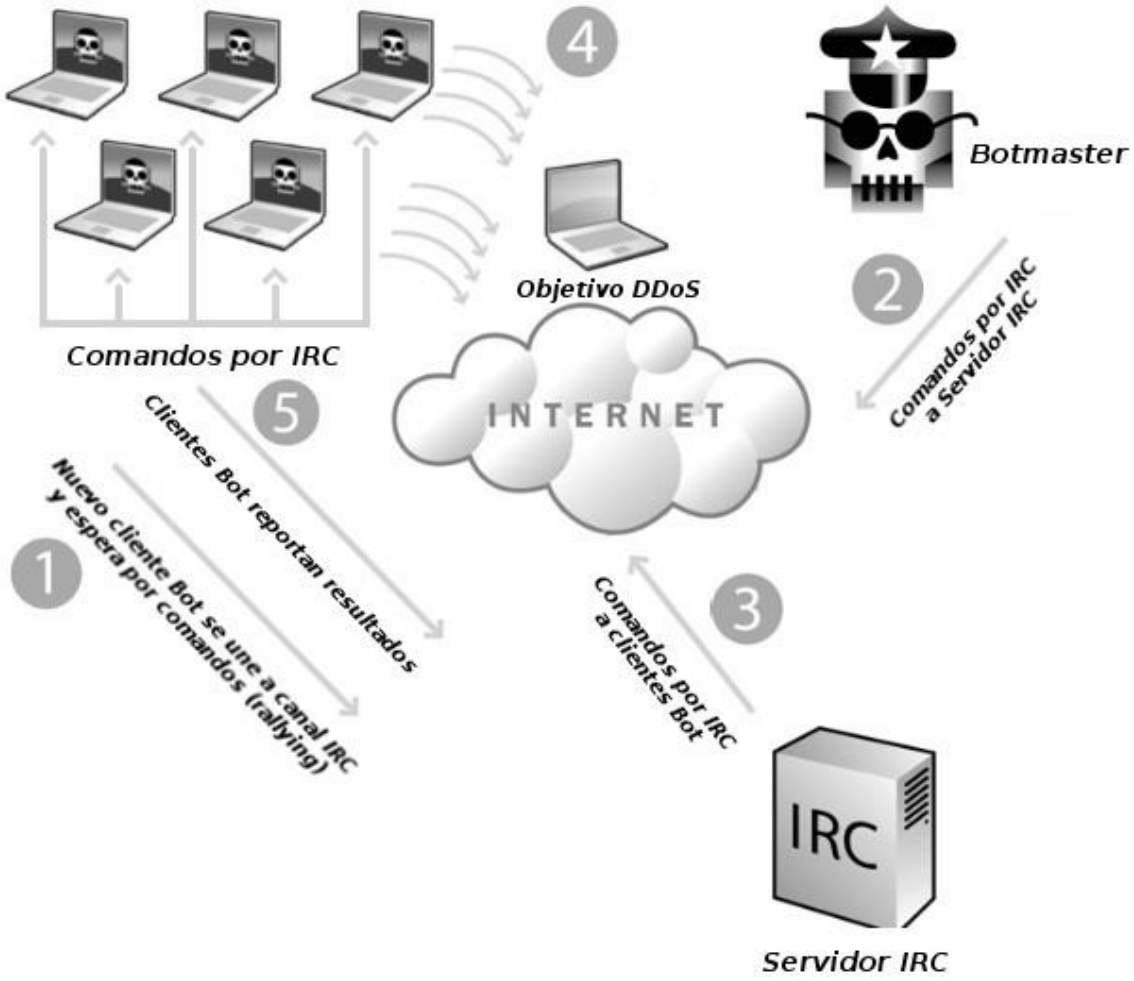


Botnets_Una definición

"una red de sistemas interconectados, bajo el control expreso de una entidad remota, cada uno de los cuales es vulnerado por uno o más bots, y usado para realizar tareas y ataques que pueden ser llevados a cabo de forma más efectiva por muchas máquinas conectadas que por las máquinas aisladas"

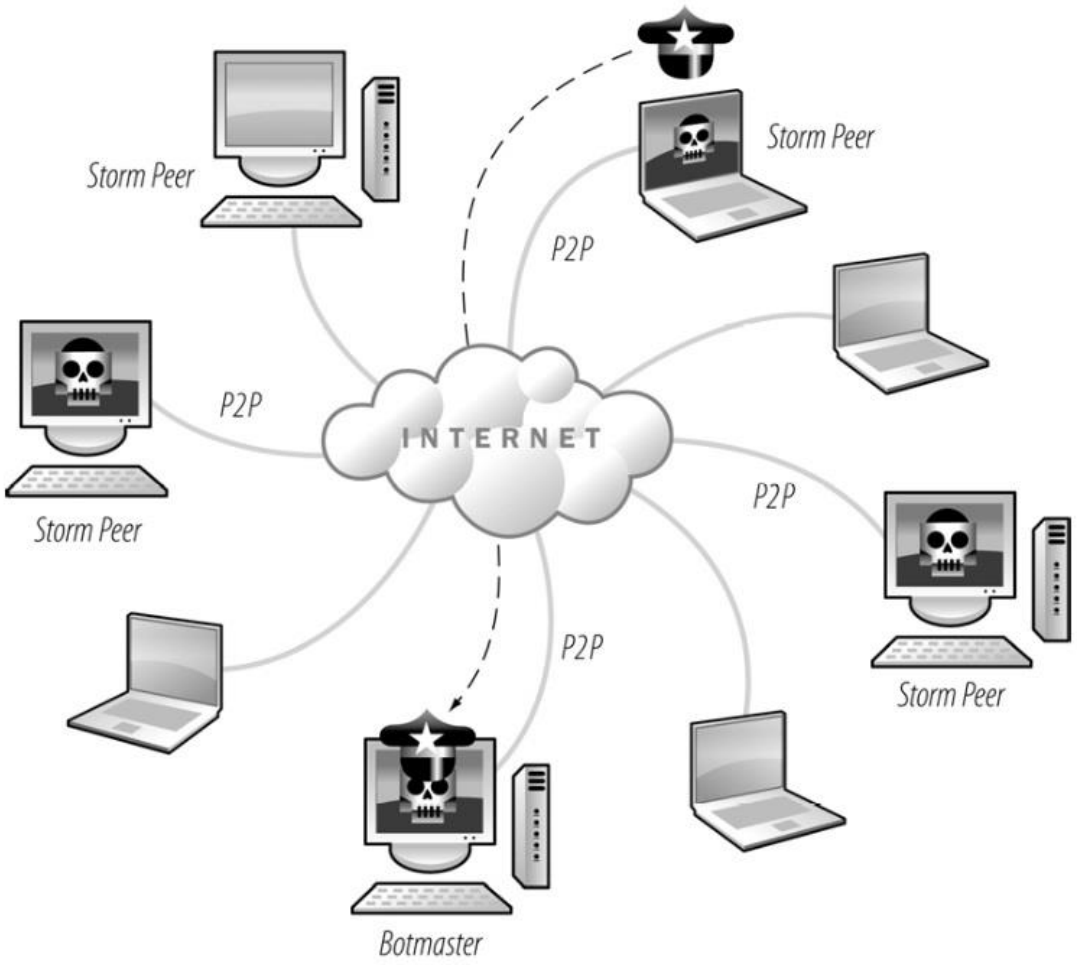
Command&Control

C&C por IRC



Command&Control

C&C por P2P



Command&Control

C&C por P2P

- Peers
- Botmaster determina servidores
- Módulos distribuidos. Listas de archivos
- Distribución de comandos: pull / push

C&C por HTTP

- Modelo centralizado (similar IRC)
- Comunicación bajo demanda
- Se mezcla con tráfico de Internet
- Kits listos, fáciles de usar

Command&Control

C&C por HTTP

Otras tecnicas

DNS Dinámico_Fast Flux

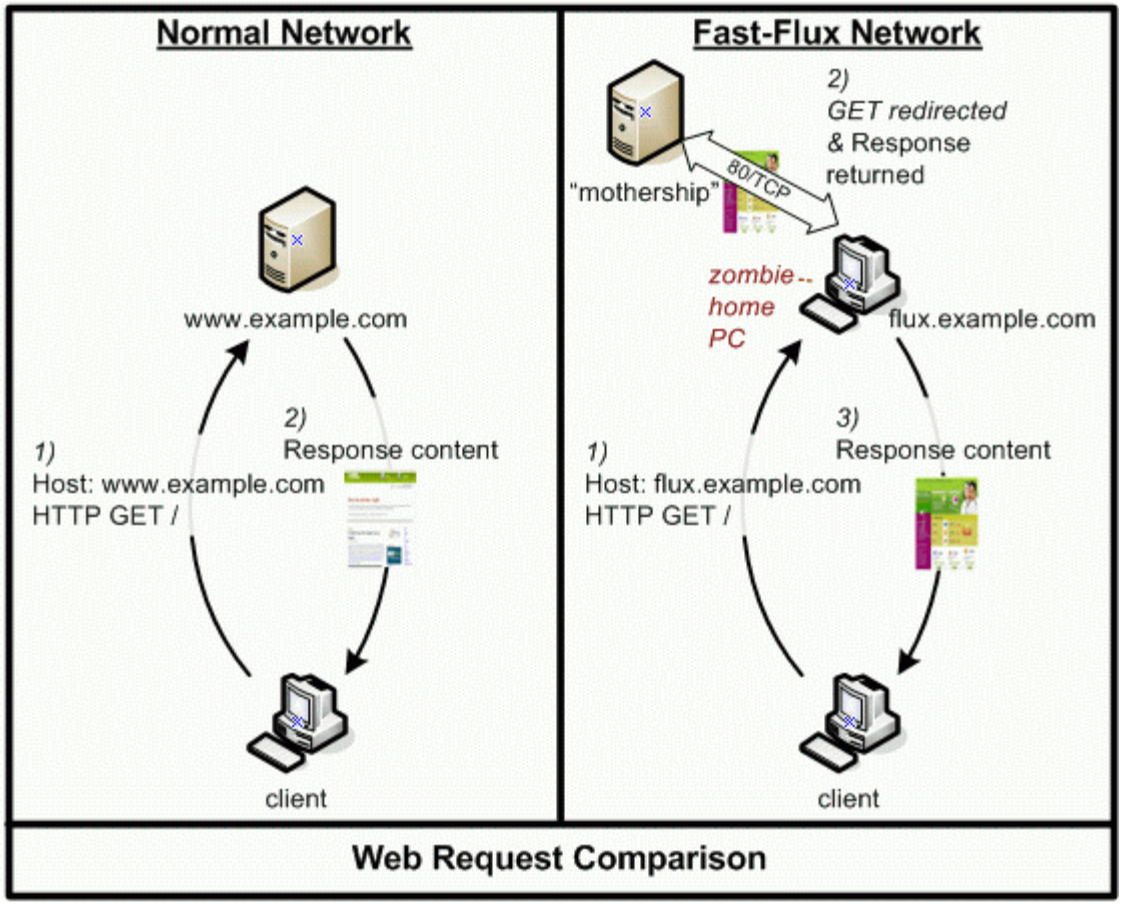
- Asignar pool de IPs a un dominio
- Rotar rápidamente
- Utilizar varios nombres de dominio

Proxies

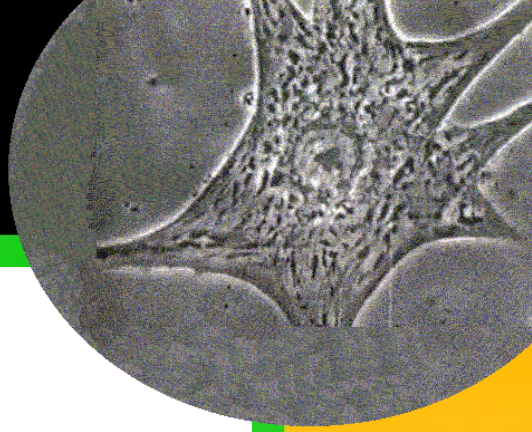
- Comunicación indirecta con los servidores
- Se pueden utilizar varios niveles
- Promoción / Degradación

Otras tecnicas

Ejemplo



Ataques



>Autopropagación

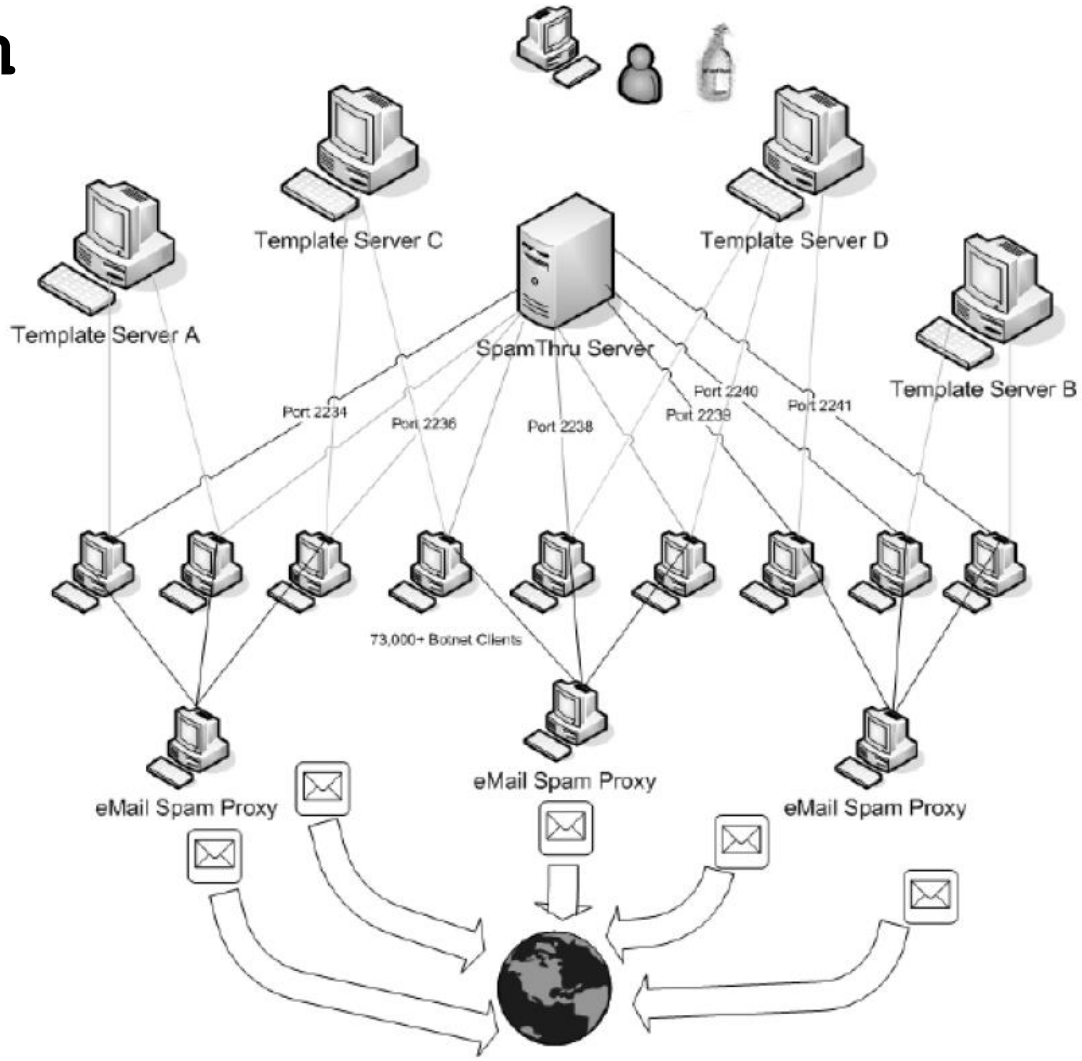
- Reclutar zombies

>Spam

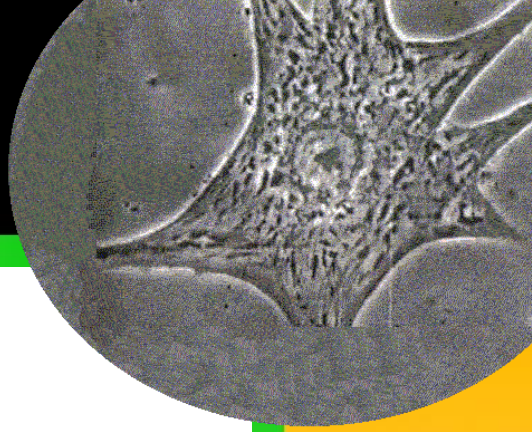
- Distintas plantillas a distintos grupos de zombies
- Proxies
- 1 respuesta cada 12.5 millones de e-mails
- 80% de e-mails son spam, 80% de botnets

Ataques

>Spam



Ataques



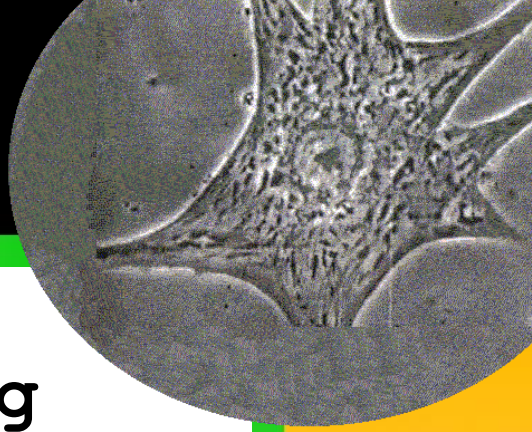
>DDoS

- Inundación
- Paquetes SYN. Conexión
- Extorsión. Alquiler

>Adware y Fraude por clicks

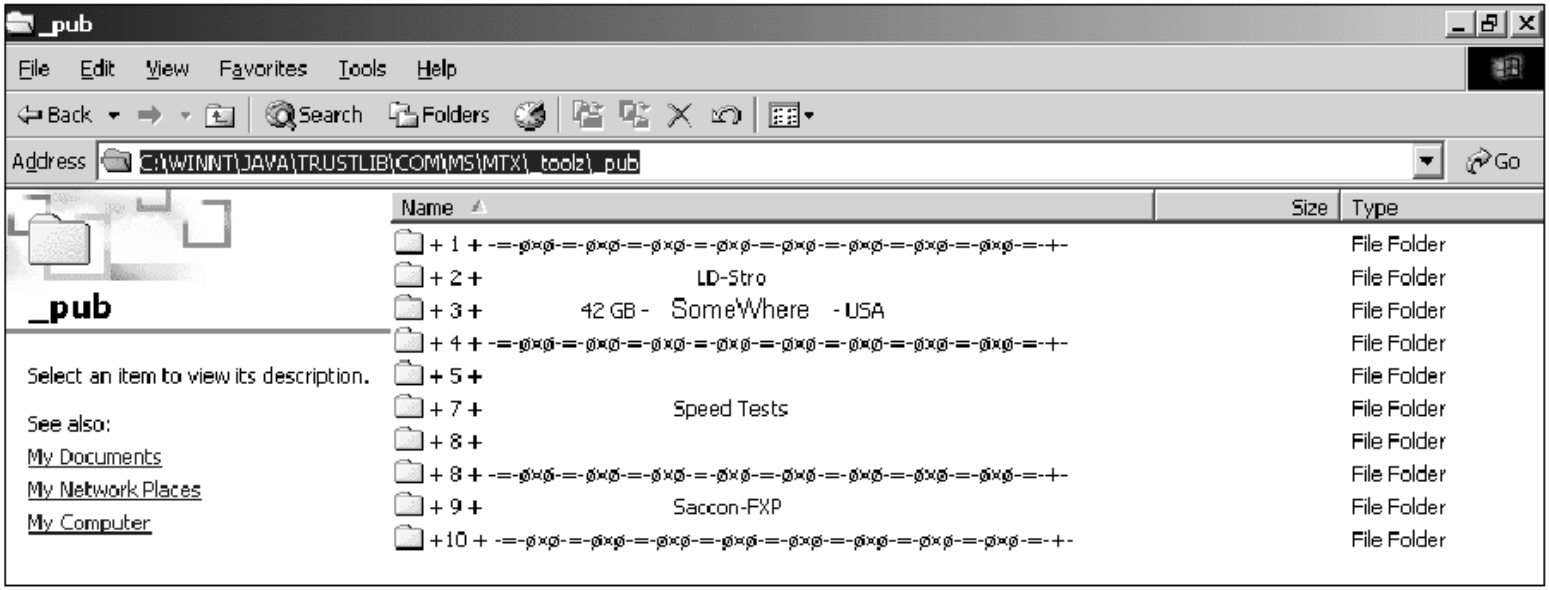
- Google AdSense
- 15% de los clicks son fraudulentos
- Pago por instalación de adware

Ataques



>**Phishing, pharming, keylogging**

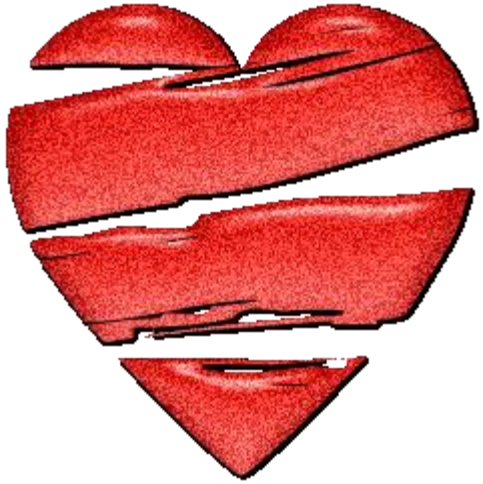
>**Almacenamiento de información ilegal**



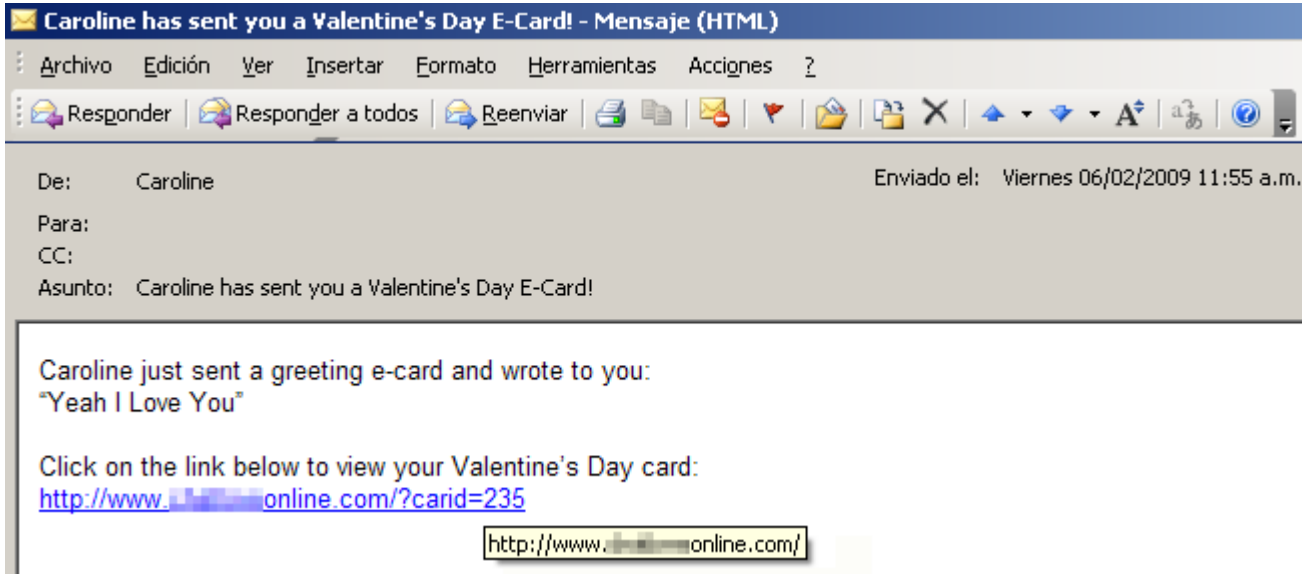
Intervenciones

2009 Waledac

- Troyano
- Esparcimiento masivo en San Valentín (2009)
- Distribuido mediante spam
- Utilizado para generar spam
- 100 000 zombies



Intervenciones



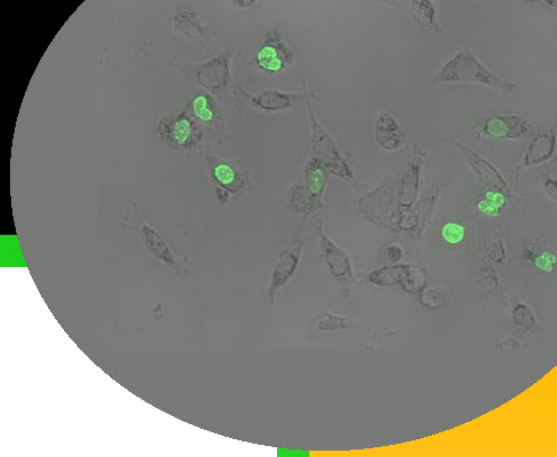
Intervenciones

Intervenciones

>Waledac

Luego de que Microsoft presentara una denuncia ante la corte estadounidense de Virginia, el 22 de febrero de 2010 el juzgado federal forzó el cierre de 277 dominios de Internet utilizados por la botnet

Intervenciones



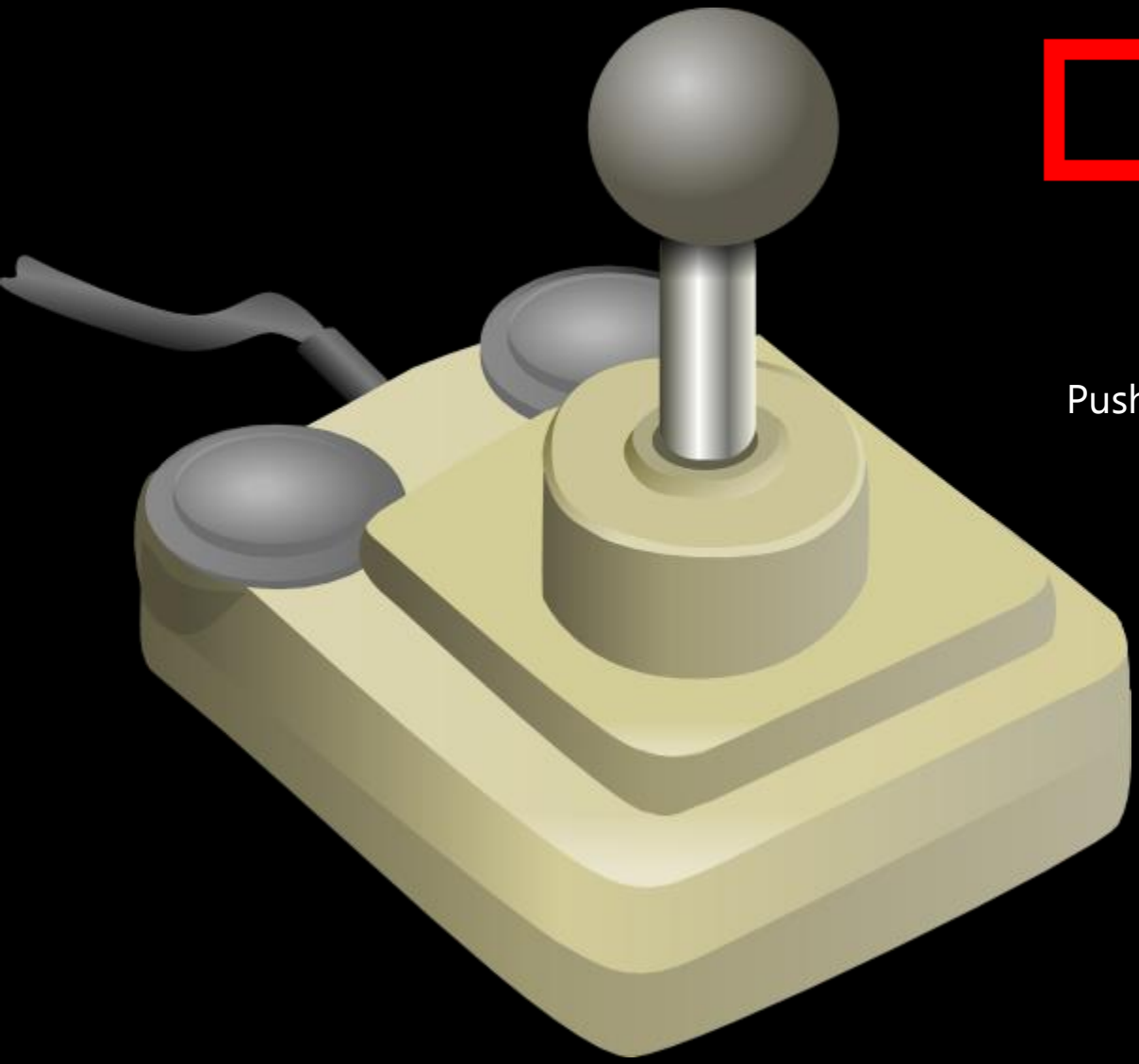
2010 Bredolab

- Difundía spam y era alquilada
- 30 millones de zombies
- Desmantelada por el gobierno holandés y profesionales de seguridad

2011 Rustock

2011 Coreflood

.
.
.



DEMO

Push any Button

Grazie
Bambini!!